Docket No.: 20162-00547-US
(PATENT)

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of:
Kazumaro Aoki et al.

Confirmation No.: 6943

Application No.: 09/463,907

Filed: February 2, 2000

Art Unit: 2131

For: DEVICE AND METHOD FOR EVALUATING RANDOMNESS OF FUNCTIONS, DEVICE AND METHOD FOR GENERATING RANDOM FUNCTION, AND RECORDED MEDIUM ON WHICH PROGRAMS FOR IMPLEMENTING THESE METHODS ARE RECORDED

Examiner: C. A. LaForgia

SUPPLEMENTAL APPEAL BRIEF

MS Appeal Brief - Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

July 19, 2006

Dear Sir:

As required under § 41.37, this supplemental brief is filed within one month of the Notification of Non-Compliant Appeal Brief mailed in this case on June 19, 2006, and is in furtherance of said Notice of Appeal.

Without arguing the impropriety of any of the Primary Examiner's objections to the originally filed Appeal Brief, this Supplemental Appeal Brief is submitted to expedite review by the BPAI and is believed to be responsive to each stated basis for objection.

No fees are believed to be due with this supplemental brief.

This brief contains items under the following headings as required by 37 C.F.R. § 41.37 and M.P.E.P. § 1206:

I. REAL PARTY IN INTEREST

The real party in interest for this appeal is Nippon Telegraph and Telephone Corporation, Tokyo, Japan.

II. RELATED APPEALS, INTERFERENCES, AND JUDICIAL PROCEEDINGS

There are no other appeals, interferences, or judicial proceedings which will directly affect or be directly affected by or have a bearing on the Board's decision in this appeal.

III. STATUS OF CLAIMS

A. Total Number of Claims in Application:

B. There are 16 claims pending in application, including multiple dependent claims.

C. Current Status of Claims

1. Claims canceled: 1-5, 7, 9-12, 17, 24, 27-30, and 33-38
2. Claims withdrawn from consideration but not canceled: none
3. Claims pending: 6, 8, 13-16, 18-23, 25-26, 31, and 32
4. Claims allowed: none
5. Claims rejected: 6, 8, 13-16, 18-23, 25-26, 31, and 32

6. Multiple dependent: 15, 16, 22, and 23

D. Claims On Appeal: 6, 8, 13-16, 18-23, 25-26, 31, and 32.

IV. STATUS OF AMENDMENTS

Applicant did not file an Amendment After Final Rejection. The claims on appeal reflect Applicants' last amendment to the claims filed on August 5, 2005.

V. SUMMARY OF CLAIMED SUBJECT MATTER

A. Overview of Applicants' Claimed Invention

A "plain-language" overview of the claimed subject matter and related background information is provided to aid in the Honorable Board's understanding of the unique and non-obvious aspects of Applicants' invention.

The claimed invention relates to an apparatus, method, and recording medium having programs recorded thereon to implement functions that are applied to a cryptographic device to evaluate whether candidate functions satisfy various randomness criteria desirable to improve cipher security.

By implementing the apparatus and method, the security of the cipher against an attack can be improved by increasing the difficulty that would be necessary to perform cryptanalysis to "break the code" of the chosen cipher.

B. Detailed Summary of Claimed Invention with Reference to the Disclosure

1. Structure Associated with "Means-Plus-Function" Limitations

Various limitations of the claims on appeal are recited as "means-plus-function" limitations under 35 U.S.C. §112, sixth paragraph. As would be readily recognized by a person with skill in the cryptographic arts, such recited devices and means may be and commonly are

implemented by an appropriately programmed computer or processor running computer code adapted to carry out the recited means and method.

The structure for any such computer-implemented means-plus-function limitations in the claims on appeal and as described below are intended to be construed as a processor and/or computer with the appropriate software adaptation to carry out the various novel and non-obvious functions, as variously claimed.

2. Reference to Specification and Drawings

In the embodiment of independent claim 1, a random function generating apparatus for a data encryption device includes input means 11 for inputting digital signals representing parameter values of each of a plurality of functions each of a composite function composed of first and second functions of different algebraic structures (see Specification at p. 18, lines 1-11, FIG. 2 elements 21, 22), and for storing the digital signals in storage means 13 (see Specification at p. 6, lines 15-23).

A candidate function generating means 12 generates candidate functions for each of the composite function formed of said first and second functions of different algebraic structures (see Specification at p. 18, lines 1-11, FIG. 2 elements 21, 22, i.e., P(x, e) and A(y, a, b)) based on the plurality of parameters stored in and read out of the storage means 13 (see Specification at p. 6, lines 20-23).

Resistance evaluating means evaluate the resistance of each of said candidate functions to a cryptanalysis (see Specification at p. 6, line 23 through p. 7, line 11; p. 7, line 20 through p. 17, line 10; FIG. 2 blocks 14a-14g).

Selecting means 15 selects the resistance-evaluated candidate functions which are highly resistant to cryptanalysis and outputs digital signals (see FIG. 1, ref. no. 17) representing selected ones of said resistance-evaluated candidate functions (see Specification at p. 7, lines 3-11).

One of the first and second functions of different algebraic structures (see FIG. 2, P(x, e) and A(y, a, b)) is resistant to each of differential cryptanalysis and linear cryptanalysis (see Specification at p. 18, lines 5-22).

In the embodiment of independent claim 13, a random function generating method for data encryption inputs digital signals representing input difference values Δx (see Specification at p. 8, lines 2-3; p. 16, lines 14-19), output mask values Γy (see Specification at p. 9, lines 18-21), and parameter values of each of a plurality of candidate functions (see Specification at p. 18, line 26 through p. 20, line 5; and FIG. 3, step S1). The digital signals are stored in storage means (FIG.1, element13), i.e., a hard disk, digital memory, or other known storage media. Various input values read out of the storage means are set for each of candidate functions S(x) of S-box and output values are calculated corresponding to the various input values x.

The output values are stored in storage means (see FIG. 1, element 16, and Specification at p. 7, lines 3-7). The resistance of each of said candidate functions to a cryptanalysis is evaluated based on the output values stored in the storage means 16. Selective candidate functions highly resistant to the various types of cryptanalysis (e.g., FIG. 1, blocks 14a-14f) are output (see Specification at p. 6, line 23 through p. 7, line 7).

The evaluation of the resistance of each candidate function to a specific type of cryptanalysis is performed by a higher-order cryptanalysis resistance evaluating step that includes calculating a minimum value of the degree of a Boolean polynomial for input bits of each of said candidate functions by which its output bits are expressed. The resistance of each candidate function to higher order cryptanalysis is evaluated based on the result of the calculation (see Specification at p.10, line 22 through p. 12, line 6). Those of the candidate functions whose resistance is higher than a predetermined first reference are retained, and the remainder are discarded (see Specification at p.20, lines 6-23 and FIG. 3, steps S3-S22, for example).

Further, a differential-linear cryptanalysis resistance evaluating step includes calculating, for every set of input difference value Δx and output mask value Γy of each candidate function $S(x)$, a number of input values x for which the inner product of $(S(x)+S(x+\Delta x))$ and the output mask value Γy is 1 (see Specification at p. 16, lines 6-20).

The resistance of the candidate function to differential-linear cryptanalysis is evaluated based on the result of the calculation, and those of the candidate functions whose resistance is higher than a predetermined second reference are retained, and others are discarded (see Specification at p.18, lines 5-11, and FIG. 3, step S12).

A partitioning-cryptanalysis resistance evaluating step divides all input values of each candidate function and the corresponding output values into input subsets and output subsets (see Specification at p. 14, lines 12-23). An imbalance of the relationship between the input subset and the output subset is calculated with respect to their average corresponding relationship. The resistance of each candidate function to partitioning cryptanalysis is evaluated based on the result of the calculation. Those of the candidate functions whose resistance is higher than a predetermined third reference are retained, and others are discarded (see Specification at p. 14, line 24 through p. 16, line 4; FIG. 3, step S15).

Interpolation-cryptanalysis resistance is evaluated by expressing an output value y as $y = f_k(x)$ for an input value x and a fixed key k using a polynomial over a Galois field which is composed of elements equal to a prime p or a power of the prime p. A number of terms of the polynomial are counted. The resistance of the candidate function to interpolation cryptanalysis is evaluated, ; and leaving those of said candidate functions whose resistance is higher than a predetermined fourth reference are retained, and others are discarded (see Specification at p. 12, line 7 through p. 13, lines 16; FIG. 3, step S18).

The candidate functions are each a composite function composed of first and second functions of different algebraic structures, and at least one of the first and second functions is

resistant to differential cryptanalysis and linear cryptanalysis (see Specification at p. 18, lines 1-11, FIG. 2 elements 21, 22).

In the embodiment of independent claim 20, a recording medium has a random function generating method for data encryption encoded thereon as a computer program (see Specification at p. 24, lines 10-15). When executed, the program sets values as each parameter for candidate functions S(x) and calculates output values corresponding to various input values (see Specification at p. 8, lines 2-8). Output values are stored in storage means 13, e.g., hard disk and/or digital memory (see Specification at p. 6, lines 15-23).

The resistance of each of the candidate functions to a cryptanalysis based is evaluated based on the output values stored in the storage means. Candidate functions that are highly resistant to the cryptanalysis are selectively output (see Specification at p. 6, line 23 through p. 7, line 11; p. 7, line 20 through p. 17, line 10; FIG. 2, blocks 14a-14g).

The resistance of each of the candidate functions to a cryptanalysis based is evaluated by several processes.

Higher-order cryptanalysis resistance is evaluated by calculating a minimum value of the degree of a Boolean polynomial for input bits of each of the candidate functions by which its output bits are expressed. The resistance of each candidate function to higher order cryptanalysis is evaluated based on the result of the calculation. Those of the candidate functions whose resistance is higher than a predetermined first reference are retained, and others are discarded (see Specification at p. 10, line 17 through p. 12, line 6).

Differential-linear cryptanalysis resistance is evaluated by calculating, for every set of input difference value Δx and output mask value Γy of each candidate function S(x), a number of input values x for which the inner product of $(S(x)+S(x+\Delta x))$ and the output mask value Γy is 1. The resistance of the candidate function to differential-linear cryptanalysis is evaluated based on the result of the calculation. Those of the candidate functions whose resistance is higher than a

predetermined first reference are retained, and others are discarded (see Specification at p. 16, line 5 through 17, line 10, FIG. 3, step S12).

Partitioning-cryptanalysis resistance is evaluated by dividing all input values of each candidate function and the corresponding output values into input subsets and output subsets. An imbalance of the relationship between the input subset and the output subset is calculated with respect to their average corresponding relationship. The resistance of each candidate function to the partitioning cryptanalysis is evaluated based on the result of the calculation. Those of the candidate functions whose resistance is higher than a predetermined first reference are retained, and others are discarded (see Specification at p. 13, line 17 through p. 16, line 4; FIG. 3, step S15).

Interpolation-cryptanalysis resistance is evaluated by expressing an output value y as $y = f_k(x)$ for an input value x and a fixed key k using a polynomial over a Galois field which is composed of elements equal to a prime p or a power of the prime p. A number of terms of the polynomial are counted. The resistance of the candidate function to interpolation cryptanalysis is evaluated. Those of the candidate functions whose resistance is higher than a predetermined first reference are retained, and others are discarded (see Specification at p. 12, line 7 through p. 13, p. 16; FIG. 3, step S18).

The candidate functions are a composite function composed of first and second functions of different algebraic structures, and at least one of the first and second functions is resistant to differential cryptanalysis and linear cryptanalysis(see Specification at p.18, lines 1-11, FIG. 2 elements 21, 22).

VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

A. §102(b) Anticipation Rejection of claim 6 by Kim et al. (US 5,796,837)

B. §103(a) Unpatentability Rejection of claims 8, 13-16, 18-23, 25-26, and 31-32 over Kim et al. (US 5,796,837) in view of "The Interpolation Attack on Block Ciphers" by Jakobsen et al. ("Jakobsen"), "Partitioning Cryptanalysis" by Harpes ("Harpes"), and "Differential-Linear Cryptanalysis" by Langford et al. ("Langford")

Although headings "A" and "B" immediately above represent the only two explicit statements of rejection in the Final Rejection, the Examiner appears to somehow invoke additional references in the detailed action. All claims on appeal stand rejected based upon the above two rejections.

However, in the final rejection of claims 14 and 21, it appears that another reference may be invoked, i.e., "Block Cipher - Analysis, Design and Application", by Lars Knudsen; as well as in the rejection of claim 23, "Markov Ciphers and Differential Cryptanalysis", by Xuejia Lai.

Based upon the unclear form of the detailed discussion of the rejections and their apparent difference from the explicit statement of the rejection, Appellants are uncertain as to the complete formulation of what appear to be additional grounds of final rejection.

Accordingly, this Brief responds to the rejections of the claims on appeal as set forth in the explicit statements of the rejections as noted above.

VII. ARGUMENT

A. The anticipation rejection by Kim et al. (US 5,796,837) is deficient, as the applied art does not disclose all the limitations in claim 6, particularly the recited "candidate functions each of said composite function formed of said first and second functions of different algebraic structures"

1. The applied art does not teach or suggest all the claim limitations

Appellants note that anticipation requires the disclosure, in a prior art reference, of each and every limitation as set forth in the claims.[1] There must be no difference between the claimed invention and reference disclosure for an anticipation rejection under 35 U.S.C. §102.[2] To properly anticipate a claim, the reference must teach every element of the claim.[3] "A claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference".[4] "The identical invention must be shown in as complete detail as is contained in the ...claim."[5] In determining anticipation, no claim limitation may be ignored.[6] The applied art does not meet this threshold burden.

The Examiner asserts that Kim et al. discloses all the claimed limitations. Appellants respectfully disagree, as discussed below.

Discussion of the Deficiencies of Kim et al.

The Examiner's reliance upon Kim et al. is completely mistaken, *inter alia*, with respect to the claimed composite function constituting an S-box. Although an S-box is represented by S(x) in Kim et al., the word "function" is not found in any portion of Kim et al., and specifically silent on use of a composite function in the manner claimed by Appellants.

---

[1] *Titanium Metals Corp. v. Banner*, 227 USPQ 773 (Fed. Cir. 1985).
[2] *Scripps Clinic and Research Foundation v. Genentech, Inc.*, 18 USPQ2d 1001 (Fed. Cir. 1991).
[3] *See* MPEP § 2131.
[4] *Verdegaal Bros. v. Union Oil Co. of Calif.*, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987).
[5] *Richardson v. Suzuki Motor Co.*, 9 USPQ2d 1913, 1920 (Fed. Cir. 1989).
[6] *Pac-Tex, Inc. v. Amerace Corp.*, 14 USPQ2d 187 (Fed. Cir. 1990).

Kim et al. discloses various cryptanalysis methods for evaluation on S-boxes, each given as a table such as shown in Fig. 5, for example (see also similar eight tables in Figs. 14A-14H which are to be used for eight S-boxes 305-307 in Fig. 3). FIG. 6 shows a flowchart for conducting evaluation on S-boxes with respect to differential cryptanalysis (col. 4, lines 10-11).

FIGS. 7-10 show flowcharts for conducting evaluation of S-boxes with respect to linear cryptanalysis (col. 4, lines 3 1-33, 41-43, 51-53 and 63-65). According to Fig. 6, steps 606 and 607 check to determine if S(x) is equal to S(x ⊕ (ll efg 0). If the result is YES, the table representing an S-box does not satisfy the required condition (see col. 4, lines 12-18).

In the REMARKS in the response filed on October 28, 2004, Appellants explained that "the equation in column 4, lines 25-30 of Kim et al. patent relates to evaluation for linear cryptanalysis" and "may correspond to the equation (4) on page 9 of the present application." That is, the equation in col. 4, lines 25-30 of Kim et al. is ***not*** a function of an S-box. Rather, ***the equation is an evaluation measure for evaluating an S-box***.

In the REMARKS of the response filed on August 5, 2005, Appellants further explained that "column 4 of Kim relates to (1) the process for checking whether the S-box satisfies the condition Dl related to the differential cryptanalysis (col. 4, lines 10-11), and (2) conditions Ll to L5 related to the linear cryptanalysis (col. 4, lines 31, 41, 51, 63)", and that "Kim patent discloses nothing about forming an S-box by a composite function composed of two different algebraic structures."

Thus, it is apparent that the Examiner's reasoning in the paragraphs 4-10 of the Final Official Action is based on a completely mistaken interpretation of Kim et al.

During the personal interview between Examiner LaForgia and Appellants' representative on January 18, 2006, and as reflected in the Interview Summary (PTOL-413) of the same date, the Examiner asserted that Kim et al. discloses a composite function composed of first and second functions of different algebraic structures.

The Examiner cited col. 4, lines 1-30 and FIG. 6 as support for his position regarding the recited "first and second functions of different algebraic structures", in particular, he believes that the equation at col. 4, line 28, i.e., the equation

$$NS(\alpha, \beta) = \#\{x \varepsilon Z_2^{64}\ x\alpha = S(x) \bullet \beta\} - 32$$

discloses the claimed "plurality of functions each of a composite function composed of first and second functions of different algebraic structures."

This is an erroneous reading of the reference. Kim et al. disclose at col. 4, lines 19-30 that $NS(\alpha, \beta)$ is merely a computed linear distribution table of the substitution-box. Further, it is clear from just looking at the equation for $NS(\alpha, \beta)$ that it is not composed of ***two functions*** of ***different algebraic structures***.

This deficiency of Kim et al. is even more apparent when the claim limitation is considered in light of Appellants' disclosure relating to the limitation at issue, i.e., FIG. 2, P(x, e) and A(y, a, b) and the Specification at p. 18, lines 5-22, which disclose that a composite function is used.

Specific Deficiencies of Kim et al.

The applied art does not disclose a random function generating apparatus for a data encryption device that includes, among other features, "...inputting digital signals...of each of a plurality of functions each of a composite function composed of first and second functions of different algebraic structures...means for generating candidate functions each of said composite function formed of said first and second functions of different algebraic structures...wherein one of said first and second functions of different algebraic structures is resistant to each of differential cryptanalysis and linear cryptanalysis.

Therefore, since the applied art does not disclose each limitation of claim 6, reversal of the rejection and allowance of claim 6 by the Honorable Board is respectfully requested.

2. The Examiner's contention that it is "'well-known' to use mathematical functions in choosing good, secure S-boxes" ignores Appellants' claimed implementation of a *composite* function, and this contention is largely irrelevant to Appellants' claimed limitation

In the "Response to Arguments" section of the Final Official Action, the Examiner appears to take "official notice" that it is "well known to use mathematical functions in choosing good, secure S-boxes…[as] supported by **Applied Cryptography** by Bruce Schneier…on pages 349-351…[where it is stated] that math-made S-boxes are chosen according to mathematical principles so that they have proven security against differential and linear cryptanalysis and good diffusive properties…[and which] is further supported by **Differentially uniform mappings for cryptography**, which provides proof of algebraic functions providing for secure s-boxes that are secure against differential and linear cryptanalysis with good diffusive properties…[and that therefore], Kim discloses generating S-boxes using mathematical functions."

Whether or not the Examiner's characterizations of these non-cited articles or texts are technically correct, it is clear from a reading of the indicated portion of these documents that none teach or suggest use of a ***composite function composed of first and second functions of different algebraic structures***, as claimed.

Accordingly, reversal of the anticipation rejection and allowance of independent claim 6 by the Honorable Board are respectfully requested.

B. The unpatentability rejection of claims 8, 13-16, 18-23, 25-26, and 31-32 over Kim et al. (US 5,796,837) in view of "The Interpolation Attack on Block Ciphers" by Jakobsen et al. ("Jakobsen"), "Partitioning Cryptanalysis" by Harpes ("Harpes"), and "Differential-Linear Cryptanalysis" by Langford et al. ("Langford") is deficient, as the applied art at least does not teach or suggest all the limitations in independent claims 13 and 20, particularly the recited "composite function formed of first and second functions of different algebraic structures"

1. The applied art does not teach or suggest all the claim limitations

At the outset, Applicant notes that, to establish a *prima facie* case of obviousness, three basic criteria must be met. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference must teach or suggest all the claim limitations.[7] Further, the teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art, not in applicant's disclosure.[8]

The deficiencies of Kim et al. were discussed, *supra*, with respect to the anticipation rejection of independent claim 6. The cited deficiency is equally pertinent to the unpatentability rejection of claim 8, independent method claim 13, and independent recording medium claim 20.

The secondary references combined with Kim et al. do not make up for the noted deficiencies of Kim et al. in either of independent claims 13 and 20 and claims depending therefrom.

---

[7] *See* MPEP §2143.

[8] *In re Vaeck*, 947 F.2d 488, 20 USPQ2d 1438 (Fed. Cir. 1991) and *See* MPEP §2143.

Discussion of Jakobsen, Harpes, and Langford

Harpes teaches partitioning cryptanalysis and calculation of imbalance as an evaluation measure. Jakobsen teaches how to conduct high-order differential cryptanalysis and interpolation-cryptanalysis. Langford teaches how to conduct differential-linear cryptanalysis.

However, none of these references make up for the previously identified deficiencies of Kim et al., discussed above with respect to independent claim 6, and essentially identical in key respects to limitations found in independent claims 13 and 20. Kim teaches evaluation of resistance of S-boxes to differential cryptanalysis and linear cryptanalysis, but does not teach anything about an S-box formed of a composite function composed of two different algebraic structures.

Jakobsen states in the abstract that "ciphers of low non-linear order are vulnerable to attacks based on high-order differentials" and also that the new interpolation attack "is useful for attacking ciphers using simple algebraic functions as S-boxes."

Harpes states in the abstract that iterated block ciphers have such a weakness that "the last-round inputs are non-uniformly distributed over the blocks of the second partition."

These statements quoted from the abstracts of the cited references are submitted as being far too general, and it would be insufficient to deduce therefrom three concrete evaluation measures for evaluating resistance of S-boxes to the three cryptanalysis attacks as variously recited in claims 13 and 20.

Further, Langford builds on a new attack technique, differential-linear cryptanalysis from the known differential and linear cryptanalysis, achieving reduction of the amount of required text. However, Langford does not suggest any evaluation measure such as a number of input values x which satisfy $(S(x)+S(x+\Delta x))\bullet\Gamma y=1$ for evaluating S-boxes.

Thus, none of Kim, Jakobsen, Harpes or Langford teaches ***anything*** about evaluation of resistance of an S-box formed of a composite function composed of two algebraic structures.

Regarding the Examiner's assertion in paragraphs 20-26 of the Final Official Action, arguably, steps (o), (a), (b) and (c) in independent method claim 13 are suggested by Kim et al. However, recited steps (c-1) to (c-4) are clearly not taught or suggested by any one of Kim et al., Jakobsen, Harpes, or Langford.

Regarding the Examiner's assertions in paragraphs 27-29 of the Final Official Action, the Examiner has confused linear cryptanalysis, differential cryptanalysis and differential-linear cryptanalysis.

Knudsen describes differential cryptanalysis and linear cryptanalysis but does not describe differential-linear cryptanalysis. Equation 6.2 on page 117 of Knudsen is defined with respect to the <u>linear cryptanalysis</u>, and this equation is certainly equivalent to the equation in col. 4, lines 25-30 of Kim et al. In the equation of either references, the number of inputs x which satisfy $x\alpha=S_i(x)\beta$ are counted. This equation is essentially equivalent to equation (4) on page 9, line 22 of the present application, which is recited in connection with the <u>linear cryptanalysis</u> as explained in the previous Remarks filed on October 28, 2004.

Contrary to equation 6.2 of Knudsen, the equation recited in claim 14 relates to the <u>differential-linear cryptanalysis</u>. In the equation recited in claim 14, a number of input differences Δx which satisfy $(S(x)+S(x+\Delta x))\bullet\Gamma y=1$ are counted. Therefore, the meaning of the equation in claim 14 completely differs from the meaning of equation 6.2 in Knudsen.

Regarding the Examiner's statement in paragraph 30 of the Final Official Action, Kim et al. discloses S-box testing procedures, wherein, in the case of condition Dl related to differential cryptanalysis shown in Fig. 6, those variables x, y and efg are changed during repeated processing for each S-box, but the test condition to be satisfied, $S(x)=S(x\oplus 11\ efg\ 0)$, remains intact. In the case of condition L1 related to the linear cryptanalysis shown in Fig. 7, the linear

distribution table NS(α, β) is calculated by the equation shown in col. 4, lines 26-28 and the maximum value m in the distribution table is determined in step 703. Then, m is checked to see if it is less than 16 in step 704 (see col. 4, lines 19-40). There is no teaching or suggestion of changing this test condition in Kim et al. In the other examining procedures for conditions L2-L6 shown in Figs. 8-12, satisfaction of required conditions are checked in steps 704; 804; 905; 1011-1014, 1027-1030; 1105; and 1205; respectively, however, those test conditions are kept unchanged. Thus, the Examiner's assertion in this regard is based on an erroneous understanding of the applied art.

Regarding the Examiner's statement in paragraph 31 of the Final Official Action, and as previously explained, Kim et al. does not teach or suggest anything at all about the use of a composite function of two different algebraic structures for an S-box.

Regarding the Examiner's statement in paragraphs 32, 33 of the Final Official Action, the cited Xuejia Lai reference discloses in section 2 how to perform differential cryptanalysis on r-round iterated cipher for a selected text, wherein a (r-1) round differential (α, β) which maximizes differential probability $P(\Delta Y(r\text{-}1)=\beta|\Delta x=\alpha)$ is found. However, the differential cryptanalysis according to Xuejia Lai does not count the number of inputs x which satisfies the condition of $S(x)+S(x+\Delta x)= \Delta y$.

Specific Deficiencies of the Applied Art

<u>Claim 13</u>

In particular, the applied art, taken alone or in combination, does not teach or suggest a random function generating method for data encryption that includes, among other features, "…inputting digital signals representing input difference values Δx, output mask values Γy and parameter values of each of a plurality of candidate functions…a higher-order cryptanalysis resistance evaluating step of: calculating a minimum value of the degree of a Boolean polynomial for input bits of each of said candidate functions by which its output bits are

expressed…a differential-linear cryptanalysis resistance evaluating step of: calculating, for every set of input difference value Δx and output mask value Γy of each candidate function S(x), a number of input values x for which the inner product of (S(x)+S(x+Δx)) and said output mask value Γy is 1…a partitioning-cryptanalysis resistance evaluating step of: dividing all input values of each candidate function and the corresponding output values into input subsets and output subsets; calculating an imbalance of the relationship between the input subset and the output subset with respect to their average corresponding relationship…an interpolation-cryptanalysis resistance evaluating step of: expressing an output value y as $y = f_k(x)$ for an input value x and a fixed key k using a polynomial over Galois field which is composed of elements equal to a prime p or a power of said prime p…***wherein said candidate functions are each a composite function composed of first and second functions of different algebraic structures***, at least one of said first and second functions being resistant to said differential cryptanalysis and said linear cryptanalysis", as recited in independent claim 13.

Claim 20

The applied art, taken alone or in combination, does not teach or suggest a recording medium having recorded thereon a random function generating method for data encryption as a computer program, wherein the program includes, among other features, steps for "…setting various values as each parameter for candidate functions S(x) and calculating output values corresponding to various input values…evaluating resistance of each of said candidate functions to a cryptanalysis…wherein said [said evaluating resistance includes]…a higher-order cryptanalysis resistance evaluating step of: calculating a minimum value of the degree of a Boolean polynomial for input bits of each of said candidate functions by which its output bits are expressed…a differential-linear cryptanalysis resistance evaluating step of: calculating, for every set of input difference value Δx and output mask value Γy of each candidate function S(x), a number of input values x for which the inner product of (S(x)+S(x+Δx)) and said output mask value Γy is 1…a partitioning-cryptanalysis resistance evaluating step of: dividing all input values of each candidate function and the corresponding output values into input subsets and output

subsets…and an interpolation-cryptanalysis resistance evaluating step of: expressing an output value y as $y = f_k(x)$ for an input value x and a fixed key k using a polynomial over Galois field which is composed of elements equal to a prime p or a power of said prime p…wherein said candidate functions are ***each a composite function composed of first and second functions of different algebraic structures***…", as recited in independent claim 20.

Appellants submit that the Examiner has therefore not established a *prima facie* case of unpatentability.

Accordingly, since the applied art does not teach or suggest all the claim limitations, reversal of the rejections and allowance of claims 8, 13-16, 18-23, 25-26, and 31-32 by the Honorable Board are respectfully requested.

2. The Examiner has not established the proper motivation to combine the references in the manner suggested

An essential evidentiary component of an obviousness rejection is a teaching or suggestion or motivation to combine the prior art references.[9] Combining prior art references without evidence of a suggestion, teaching or motivation simply takes the inventors' disclosure as a blueprint for piecing together the prior art to defeat patentability – the essence of hindsight.[10]

"There are three possible sources for a motivation to combine references: the nature of the problem to be solved, the teachings of the prior art, and the knowledge of persons of ordinary skill in the art."[11] Further with regard to the level of skill of practitioners in the art, there is nothing in the statutes or the case law which makes "that which is within the capabilities of one

[9] *C.R. Bard, Inc. v. M3 Systems, Inc.*, 48 USPQ2d 1225 (Fed. Cir. 1998)
[10] *Interconnect Planning Corp. v. Feil*, 227 USPQ 543 (Fed. Cir. 1985)
[11] *See* MPEP §2143.01, citing *In re Rouffet*, 149 F.3d, 1350, 1357, 47 USPQ2d 1453, 1457-8 (Fed. Cir. 1998).

skilled in the art" synonymous with obviousness.[12] The level of skill in the art cannot be relied upon to provide the suggestion to combine references.[13]

Basically, the three secondary references (Harpes, Jakobsen, and Langford) are directed to ***cryptanalysis methods for attacking ciphers***, and do not teach or suggest any evaluation measure ***for evaluating resistance of S-boxes*** to such attacks. In other words, these references do not teach or suggest seeking S-boxes which are resistant to various known cryptanalysis attacks.

In stark contrast, the Appellants' claimed invention seeks to meet the objective of determining S-boxes which are resistant to various cryptanalysis attacks, and particularly seeks to determine an S-box formed of a ***composite function which is composed of two different algebraic structures***.

Accordingly, since the only motivation to combine the references in the manner suggested by the Examiner is by use of impermissible hindsight using Appellants' disclosure against them, Appellants submit that the Examiner has not established a *prima facie* case of unpatentability, and that the unpatentability rejections should be reversed by the Honorable Board.

[12] *Ex parte Gerlach and Woerner*, 212 USPQ 471 (PTO Bd. App. 1980).
[13] *See* MPEP §2143.01, citing *Al-Site Corp. v. VSI Int'l Inc.*, 50 USPQ2d 1161 (Fed. Cir. 1999).

VIII. CONCLUSION

In view of the above, Appellants submit that the Examiner has not met his burdens in rejecting appealed claims 6, 8, 13-16, 18-23, 25-26, 31, and 32, and that all rejections should be reversed by the Honorable Board.

Respectfully submitted,

By /Larry J. Hume/

Larry J. Hume
Registration No.: 44,163
CONNOLLY BOVE LODGE & HUTZ LLP
1990 M Street, N.W., Suite 800
Washington, DC 20036-3425
(202) 331-7111
(202) 293-6229 (Fax)
Attorney for Applicant

APPENDIX A

Claims Involved in the Appeal of Application Serial No. 09/463,907

6. A random function generating apparatus for a data encryption device comprising:

input means for inputting digital signals representing parameter values of each of a plurality of functions each of a composite function composed of first and second functions of different algebraic structures, and for storing them in storage means;

candidate function generating means for generating candidate functions each of said composite function formed of said first and second functions of different algebraic structures based on said plurality of parameters read out of the storage means;

resistance evaluating means for evaluating the resistance of each of said candidate functions to a cryptanalysis; and

selecting means for selecting those of said resistance-evaluated candidate functions which are highly resistant to said cryptanalysis and outputting digital signals representing selected ones of said resistance-evaluated candidate functions;

wherein one of said first and second functions of different algebraic structures is resistant to each of differential cryptanalysis and linear cryptanalysis.

8. The random function generating apparatus of claim 6, wherein said input means is adapted to input digital signals representing input difference values Δx and output mask values Γy and storing them in the storage means, and said resistance evaluating means comprises at least one of:

higher-order-differential cryptanalysis resistance evaluating means for: calculating a minimum value of the degree of a Boolean polynomial for input bits by which output bits of each of said candidate functions are expressed; and evaluating the resistance of said each candidate function to higher order cryptanalysis based on the result of said calculation;

interpolation-cryptanalysis resistance evaluating means for: expressing an output value y as $y = f_k(x)$ for an input value x and a fixed key k using a polynomial over Galois field which is composed of elements equal to a prime p or a power of said prime p; counting a number of terms of said polynomial; and evaluating the resistance of said each candidate function to interpolation cryptanalysis based on the result of said number;

partitioning-cryptanalysis resistance evaluating means for: dividing all input values of the function to be evaluated and the corresponding output values into input subsets and output subsets; calculating an imbalance of the relationships between the input subset and the output subset with respect to their average corresponding relationship; and evaluating the resistance of said candidate function to partitioning cryptanalysis based on the result of said calculation; and

differential-linear cryptanalysis resistance evaluating means for: calculating, for every set of input difference value Δx and output mask value Γy of the function $S(x)$ to be evaluated, a number of input values x for which the inner product of $(S(x)+S(x+\Delta x))$ and said output mask value Γy is 1; and evaluating the resistance of said candidate function to differential-linear cryptanalysis based on the result of said calculation.

13. A random function generating method for data encryption comprising the steps of:

(o) inputting digital signals representing input difference values Δx, output mask values Γy and parameter values of each of a plurality of candidate functions and storing them in storage means;

(a) setting various input values read out of the storage means for each of candidate functions S(x) of S-box and calculating output values corresponding to said various input values x;

(b) storing the output values in storage means; and

(c) evaluating the resistance of each of said candidate functions to a cryptanalysis based on the output values stored in said storage means, and selectively outputting candidate function highly resistant to said cryptanalysis; and

wherein said step (c) comprising:

(c-1) a higher-order cryptanalysis resistance evaluating step of: calculating a minimum value of the degree of a Boolean polynomial for input bits of each of said candidate functions by which its output bits are expressed; evaluating the resistance of said each candidate function to higher order cryptanalysis based on the result of said calculation; and leaving those of said candidate functions whose resistance is higher than a predetermined first reference and discarding the others;

(c-2) a differential-linear cryptanalysis resistance evaluating step of: calculating, for every set of input difference value Δx and output mask value Γy of each candidate function S(x), a number of input values x for which the inner product of (S(x)+S(x+Δx)) and said output mask value Γy is 1; evaluating resistance of said candidate function to differential-linear cryptanalysis based on the result of said calculation; and leaving those of said candidate functions whose resistance is higher than a predetermined second reference and discarding the others;

(c-3) a partitioning-cryptanalysis resistance evaluating step of: dividing all input values of each candidate function and the corresponding output values into input subsets and output subsets; calculating an imbalance of the relationship between the input subset and the

output subset with respect to their average corresponding relationship; evaluating the resistance of said each candidate function to said partitioning cryptanalysis based on the result of said calculation; and leaving those of said candidate functions whose resistance is higher than a predetermined third reference and discarding the others; and

(c-4) an interpolation-cryptanalysis resistance evaluating step of: expressing an output value y as $y = f_k(x)$ for an input value x and a fixed key k using a polynomial over Galois field which is composed of elements equal to a prime p or a power of said prime p; counting a number of terms of said polynomial; evaluating the resistance of said candidate function to interpolation cryptanalysis; and leaving those of said candidate functions whose resistance is higher than a predetermined fourth reference and discarding the others;

wherein said candidate functions are each a composite function composed of first and second functions of different algebraic structures, at least one of said first and second functions being resistant to said differential cryptanalysis and said linear cryptanalysis.

14. The random function generating method of claim 13, wherein:

said differential-linear-cryptanalysis resistance evaluating step (c-2) includes a step of: calculating the following equation for every set of said input difference value Δx except 0 and said output mask value Γy except 0

$$\xi_S(\Delta x, \Gamma y) = \left| 2 \times \# \{ x \in GF(2)^n \,|\, (S(x) + S(x + \Delta x)) \bullet \Gamma y = 1 \} - 2^n \right|;$$

calculating a maximum value Ξ among the calculation results; and evaluating the resistance of said candidate function to said differential-linear cryptanalysis based on said maximum value Ξ; and

said partitioning cryptanalysis resistance evaluating step (3) includes a step of dividing an input value set F and an output value set G of said candidate function into u input subsets $\{F_0, F_1,$

…, F_{u-1}} and v output subsets {G_0, G_1, …, G_{v-1}}; for each partition-pair (F_i, G_i) (i = 0, …, u-1; j = 0, 1, …, v-1), calculating a maximum one of probabilities that all output values y corresponding to all input values x of the input subset F_i belong to the respective output subsets G_j (j = 0, …, v-1); calculating a measure I_S(F, G) of an average imbalance of a partition-pair (F, G) based on all maximum values calculated for all partition pairs; and evaluating the resistance of said candidate function to said partitioning cryptanalysis based on said measure.

15. The random function generating method of claim 13 or 14, wherein:

said step (c-1) includes a step of: when no candidate function remains undiscarded, easing the candidate function selecting condition by changing said first reference by a first predetermined width, and executing again the evaluation and selecting process;

said step (c-2) includes a step of: when no candidate function remains undiscarded, easing the candidate function selecting condition by changing said second reference by a second predetermined width, and executing again the evaluation and selecting process;

said step (c-3) includes a step of: when no candidate function remains undiscarded, easing the candidate function selecting condition by changing said third reference by a third predetermined width, and executing again the evaluation and selecting process; and

said step (c-4) includes a step of: when no candidate function remains undiscarded, easing the candidate function selecting condition by changing said fourth reference by a fourth predetermined width, and executing again the evaluation and selecting process.

16. The random function generating method of claim 13 or 14, further comprising:

(c-5) a differential-cryptanalysis resistance evaluating step of: calculating, for each candidate function S(x), the number of inputs x that satisfy $S(x)+ S(x+\Delta x)=\Delta y$ for every set (Δx, Δy) except $\Delta x=0$; evaluating the resistance of said each candidate function to differential

cryptanalysis based on the result of said calculation; and leaving those of said candidate functions whose resistance is higher than a predetermined fifth reference and discarding the others before said step (c-2); and

(c-6) a linear-cryptanalysis resistance evaluating step of: calculating, for each candidate function, the number of input values x for which the inner product of the input value x and its mask value Γx is equal to the inner product of a function output value S(x) and its mask value Γy; evaluating the resistance of said each candidate function to linear cryptanalysis based on the result of said calculation; and leaving those of said candidate functions whose resistance is higher than a predetermined sixth reference and discarding the others after said step (c-5).

18. The random function generating method of claim 16, wherein:

said step (c-5) includes a step of: when no candidate function remains undiscarded, easing the candidate function selecting condition by changing said fifth reference by a fifth predetermined width, and executing again the evaluation and selecting process; and

said step (c-6) includes a step of: when no candidate function remains undiscarded, easing the candidate function selecting condition by changing said sixth reference by a sixth predetermined width, and executing again the evaluation and selecting process.

19. The random function generating method of claim 14, wherein said candidate functions are each a composite function composed of at least one function resistant to said differential cryptanalysis and said linear cryptanalysis and at least one function of an algebraic structure different from that of said at least one function.

20. A recording medium having recorded thereon a random function generating method for data encryption as a computer program, said program comprising the steps of:

(a) setting various values as each parameter for candidate functions S(x) and calculating output values corresponding to various input values;

(b) storing the output values in storage means; and

(c) evaluating resistance of each of said candidate functions to a cryptanalysis based on the output values stored in said storage means, and selectively outputting candidate function highly resistant to said cryptanalysis; and

wherein said step (c) comprises:

(c-1) a higher-order cryptanalysis resistance evaluating step of: calculating a minimum value of the degree of a Boolean polynomial for input bits of each of said candidate functions by which its output bits are expressed; evaluating the resistance of said each candidate function to higher order cryptanalysis based on the result of said calculation; and leaving those of said candidate functions whose resistance is higher than a predetermined first reference and discarding the others;

(c-2) a differential-linear cryptanalysis resistance evaluating step of: calculating, for every set of input difference value Δx and output mask value Γy of each candidate function S(x), a number of input values x for which the inner product of $(S(x)+S(x+\Delta x))$ and said output mask value Γy is 1; evaluating resistance of said candidate function to differential-linear cryptanalysis based on the result of said calculation; and leaving those of said candidate functions whose resistance is higher than a predetermined second reference and discarding the others;

(c-3) a partitioning-cryptanalysis resistance evaluating step of: dividing all input values of each candidate function and the corresponding output values into input subsets and output subsets; calculating an imbalance of the relationship between the input subset and the output subset with respect to their average corresponding relationship; evaluating the resistance

of said each candidate function to said partitioning cryptanalysis based on the result of said calculation; and leaving those of said candidate functions whose resistance is higher than a predetermined third reference and discarding the others; and

(c-4) an interpolation-cryptanalysis resistance evaluating step of: expressing an output value y as y = $f_k(x)$ for an input value x and a fixed key k using a polynomial over Galois field which is composed of elements equal to a prime p or a power of said prime p; counting a number of terms of said polynomial; evaluating the resistance of said candidate function to interpolation cryptanalysis; and leaving those of said candidate functions whose resistance is higher than a predetermined fourth reference and discarding the others;

wherein said candidate functions are each a composite function composed of first and second functions of different algebraic structures, at least one of said first and second functions being resistant to said differential cryptanalysis and said linear cryptanalysis.

21. The recording medium of claim 20, wherein:

said differential-linear-cryptanalysis resistance evaluating step (c-2) includes a step of: calculating the following equation for every set of said input difference Δx except 0 and said output mask value Γy except 0

$$\xi_S(\Delta x, \Gamma y) = \left| 2\times\#\{x \in GF(2)^n \middle| (S(x) + S(x+\Delta x)) \bullet \Gamma y = 1\} - 2^n \right|;$$

calculating a maximum value Ξ among the calculation results; and evaluating the resistance of said candidate function to said differential-linear cryptanalysis based on said maximum value Ξ; and

said partitioning cryptanalysis resistance evaluating step (3) includes a step of dividing an input value set F and an output value set G of said candidate function into u input subsets $\{F_0, F_1, \ldots, F_{u-1}\}$ and v output subsets $\{G_0, G_1, \ldots, G_{v-1}\}$; for each partition-pair (F_i, G_i) (i = 0, …, u-1; j =

0, 1, ..., v-1), calculating a maximum one of probabilities that all output values y corresponding to all input values x of the input subset F_i belong to the respective output subsets G_j (j = 0, ..., v-1); calculating a measure $I_S(F, G)$ of an average imbalance of a partition-pair (F, G) based on all maximum values calculated for all partition pairs; and evaluating the resistance of said candidate function to said partitioning cryptanalysis based on said measure.

22. The recording medium of claim 20 or 21, wherein:

said step (c-1) includes a step of: when no candidate function remains undiscarded, easing the candidate function selecting condition by changing said first reference by a first predetermined width, and executing again the evaluation and selecting process;

said step (c-2) includes a step of: when no candidate function remains undiscarded, easing the candidate function selecting condition by changing said second reference by a second predetermined width, and executing again the evaluation and selecting process;

said step (c-3) includes a step of: when no candidate function remains undiscarded, easing the candidate function selecting condition by changing said third reference by a third predetermined width, and executing again the evaluation and selecting process; and

said step (c-4) includes a step of: when no candidate function remains undiscarded, easing the candidate function selecting condition by changing said fourth reference by a fourth predetermined width, and executing again the evaluation and selecting process.

23. The recording medium of claim 20 or 21, wherein said program includes at least one of:

(c-5) a differential-cryptanalysis resistance evaluating step of: calculating, for each candidate function S(x), the number of inputs x that satisfy $S(x)+S(x+\Delta x)=\Delta y$ for every set (Δx, Δy) except $\Delta x=0$; evaluating the resistance of said each candidate function to differential

cryptanalysis based on the result of said calculation; and leaving those of said candidate functions whose resistance is higher than a predetermined fifth reference and discarding the others before said step (c-2); and

(c-6) a linear-cryptanalysis resistance evaluating step of: calculating, for each candidate function, the number of input values x for which the inner product of the input value x and its mask value Γx is equal to the inner product of a function output value S(x) and its mask value Γy; evaluating the resistance of said each candidate function to linear cryptanalysis based on the result of said calculation; and leaving those of said candidate functions whose resistance is higher than a predetermined sixth reference and discarding the others after step (c-5).

25. The recording medium of claim 23, wherein:

said step (c-5) includes a step of: when no candidate function remains undiscarded, easing the candidate function selecting condition by changing said fifth reference by a fifth predetermined width, and executing again the evaluation and selecting process; and

said step (c-6) includes a step of: when no candidate function remains undiscarded, easing the candidate function selecting condition by changing said sixth reference by a sixth predetermined width, and executing again the evaluation and selecting process.

26. The recording medium of claim 21, wherein said candidate functions are each a composite function composed of at least one function resistant to said differential cryptanalysis and said linear cryptanalysis and at least one function of an algebraic structure different from that of said at least one function.

31. The random function generating method of claim 15, wherein said candidate functions are each a composite function composed of at least one function resistant to said differential cryptanalysis and said linear cryptanalysis and at least one function of an algebraic structure different from that of said at least one function.

32. The recording medium of 22, wherein said candidate functions are each a composite function composed of at least one function resistant to said differential cryptanalysis and said linear cryptanalysis and at least one function of an algebraic structure different from that of said at least one function.

APPENDIX B - EVIDENCE

NONE

No evidence pursuant to §§ 1.130, 1.131, or 1.132 or entered by or relied upon by the examiner is being submitted

APPENDIX C - RELATED PROCEEDINGS

NONE

No related proceedings are referenced in II. above, and therefore copies of decisions in related proceedings are not applicable or provided.